Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Quelle est la nature du consentement du patient dans le traitement de données médicales en droit européen?

Herveg, Jean

Published in:
Lex Medicinae

Publication date:
2008

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Herveg, J 2008, 'Quelle est la nature du consentement du patient dans le traitement de données médicales en droit européen?', *Lex Medicinae*, VOL. 10, p. 15-38.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 05. May. 2023

Separata

de

Lex Medicinae

Revista Portuguesa de Direito da Saúde

JEAN HERVEG

Coimbra Editora

Centro de Direito Biomédico

QUELLE EST LA NATURE DU CONSENTEMENT DU PATIENT DANS LE TRAITEMENT DE DONNÉES MÉDICALES EN DROIT EUROPÉEN? (*)

Jean Herveg
Centre de Recherches Informatique et Droit — University of Namur
Avocat au barreau de Bruxelles

Abstract: Le consentement du patient au traitement des données médicales n'est qu'une des hypothèses permettant de traiter des données médicales. Ces hypothèses ne constituent pas tant une autorisation qu'une présomption d'équilibre entre les intérêts en présence, que ce soit ceux du patient, du responsable du traitement, de la collectivité ou des tiers considérés individuellement. D'ailleurs, le consentement ne suffit pas toujours à autoriser leur traitement. En tout état de cause, le consentement du patient ne dispense pas du respect des autres règles applicables aux traitements de données médicales. Il faut en effet respecter les autres conditions générales de licéité, les droits de la personne concernée, les obligations de confidentialité et de sécurité, et les obligations de notification à l'autorité nationale de contrôle. En cas de risques particuliers, l'examen préalable du traitement s'impose nonobstant le consentement du patient.

Mots-clés: Privacy — Protection des données — Données médicales — Consentement.

Keywords: Privacy — Data Protection — Medical data — Consent.

Introduction

1. Les questions relatives au consentement du patient sont relativement nombreuses en droit médical. Ainsi, nous pouvons déjà citer tout ce qui concerne le consentement à l'acte médical, le consentement à la participation à un essai clinique et le consentement à la communication d'informations protégées par le secret médical, sans omettre l'euthanasie ([1]). La réglementation des traitements de don-

(*) Cet article a bénéficié de la relecture attentive du Prof. Dr Yves POULLET. Il s'inscrit dans le cadre des travaux réalisés dans les projets ACGT (Advancing Clinico-Genomics Trials on Cancer: Open GRID Services for Improving Medical Knowledge Discovery) (Integrated Project, FP6-2005-IST-026996) et WALIBI (Wireless Acquisition and LInk for Body Information) (convention Région wallonne n.° 616 449). Les opinions émises n'engagent que leur auteur.

([1]) Pour la Belgique, voyez déjà: Chr. HENNAU-HUBLET, *L'activité médicale et le droit pénal. Les délits d'atteinte à la vie, à l'intégrité et la santé des personnes*, Bibl. de la Faculté de droit de l'Université catholique de Louvain, n.° 18, Bruxelles, Bruylant, Paris, L.G.D.J., 1987; D. KIGANAHE et Y. POULLET (dir.), *Le secret professionnel*, Actes du colloque des 8 et 9 novembre 2001 organisé par l'association des juristes namurois, Bruxelles, La Charte, 2002; Y. H. LELEU (coord.), *Droit médical*, Commission Université-Palais, vol. 79, Belgique, Bruxelles, Larcier, 05/2005, p. 7; Y. H. LELEU et G. GENICOT, *Le droit médical. Aspects juridiques de la relation médecin-patient*, Belgique, Bruxelles, Ed. De Boeck Université, 2001, p. 75, n.° 92, p. 151, n.° 182, p. 226, n.° 278; H. NYS, *La médecine et le droit*, Belgique, Diegem, Kluwer, 1995, p. 125, n.° 312, p. 269, n.° 686, p. 320, n.° 830,

nées à caractère personnel a introduit la notion de consentement au traitement de données à caractère personnel relatives à sa santé (2), ce qui conduit à s'interroger sur la nature de ce consentement.

Pour répondre à cette question, il faut rappeler l'objectif, le fondement et le cadre juridique de la réglementation des traitements de données à caractère personnel en droit européen.

I. Quel est l'objectif de la réglementation des traitements de données à caractère personnel?

2. L'objectif de la réglementation des traitements de données à caractère personnel est de concilier deux éléments dont la coexistence peut paraître paradoxale, sans pour autant qu'elle soit nécessairement contradictoire. 16

Le premier élément à la base de cette réglementation est la reconnaissance de la nécessité, dans le cours des activités économiques, sociales, culturelles, individuelles et domestiques, sans distinction entre les activités publiques et privées, d'exploiter l'information relative à des personnes physiques, c'est-à-dire de traiter des données à caractère personnel. Ainsi, dans la discipline qui nous intéresse (celle relative aux soins de santé), il est souvent nécessaire, sinon indispensable, d'avoir accès aux informations relatives à la santé du patient afin de lui fournir des soins de santé appropriés. De même, il est nécessaire d'exploiter ces mêmes informations dans le but de faire progresser l'état des connaissances médicales. Il existe bien entendu de nombreuses autres raisons nécessitant de traiter les informations relatives à la santé du patient. Celles-ci ressortent du financement des soins de santé, du contrôle de la qualité du système de santé publique, de l'épidémiologie, etc. Autrement dit, ce premier élément est constitué par les intérêts, droits et libertés de la personne désireuse de traiter des données à caractère personnel.

Le second élément à la base de cette réglementation, intimement lié au premier, est qu'il faut, dans le même temps, tenir compte de la personne concernée par l'information. Il s'agit de prendre en considération les intérêts, droits et libertés de la personne concernée.

3. Fondamentalement, la prise en compte du sort de la personne concernée recouvre deux aspects qui se recoupent partiellement.

Le premier aspect de la prise en compte de la personne concernée est de nature défensive. Il s'agit de la protéger contre les conséquences négatives qui peuvent découler de l'usage qui peut être fait de cette information. Il faut la protéger contre toute atteinte à ses intérêts, droits et libertés, qui pourrait résulter du traitement de l'information qui la con-

---

p. 368, n.° 955; E. THIRY (coord.), *Actualités de droit médical. Procédures disciplinaire et administrative. Information du patient et responsabilité du médecin. Le dossier du patient*, Belgique, Bruxelles, Bruylant, 2006; E. THIRY (coord.), *Actualités de droit familial et de droit médical*, Belgique, Bruxelles, Bruylant, 2007, p. 3. En ce qui concerne d'autres pays, voyez not.: A. M. DUGUET (coord.), *Droit et éthique de la recherche médicale. Originalité de la législation française, limites et questions éthiques*, Séminaire d'actualité de droit médical, France, Bordeaux, Les Etudes Hospitalières, 2004; B. R. FURROW, Th. L. GREANEY, S. H. JOHNSON, T. S. JOST et R. L. SCHWARZ, *Health Law*, 2e éd., USA, Minnesota, St Paul, West Group, Hornbook Series, 2000, p. 260, § 6-1, p. 310, § 6-9, p. 335, § 6-15, p. 337, § 6-16, p. 339, § 6-17, p. 392, § 7-6, p. 819, § 16-1, p. 984, § 21-6; I. KENNEDY et A. GRUBB, *Medical Law*, 3e éd. par A. GRUBB, U. K., Royaume-Uni, Londres, Reed Elsevier, Lexis Nexis, Butterworths, 2000, p. 575, p. 1047, p. 1084, p. 1708, p. 1907; J. K. MASON, RA MCCALL SMITH et G. T. LAURIE, *Law and Medical Ethics*, 6e éd., U.K., Londres, Reed Elsevier, Lexis Nexis, Butterworths, 2002, p. 309, n.° 10.1, p. 586, n.° 19.38, p. 242, n.° 8.7, p. 528, n.° 18.

(2) Ce qui vise la notion de données médicales.

cerne. Pour prendre un exemple, la communication d'informations relatives à la santé du patient à des personnes «non autorisées» est de nature à l'exposer à des risques de discriminations à l'emploi, au crédit, au logement, etc. Il s'agit donc de prendre les mesures appropriées pour prévenir l'avènement de ces conséquences indésirables. En droit, cette protection s'exprime au travers des conditions imposées au responsable du traitement pour qu'il puisse traiter des données à caractère personnel, et ce, afin d'éviter qu'il ne porte atteinte aux intérêts, droits et libertés de la personne concernée.

Le second aspect de la prise en compte de la personne concernée est de nature plus dynamique. Il s'agit d'assurer son droit à la maîtrise de son image informationnelle, c'est-à-dire, en quelques mots, son droit de savoir ce qui est su d'elle et ce qui en est fait, ainsi que de pouvoir influer sur l'usage de l'information qui la concerne. Ainsi, par exemple, la personne concernée peut consentir au traitement de données à caractère personnel qui la concerne. Elle dispose aussi d'un droit d'accès, de rectification, et d'opposition. Il s'agit donc de prendre les mesures appropriées pour garantir ce droit à la maîtrise de son image informationnelle, cette autodétermination informationnelle. Dans la réglementation, cette maîtrise se manifeste au travers de la mise en place des droits reconnus à la personne concernée lors du traitement de l'information qui la concerne.

Ces deux aspects se recoupent dans la mesure où la mise en œuvre des droits de la personne concernée ne s'envisage utilement que dans le respect des conditions imposées au responsable du traitement pour le traitement des données à caractère personnel, et inversement.

4. En résumé, le traitement d'informations relatives à des personnes physiques est très fréquemment nécessaire, voire indispensable, pour de multiples raisons. Mais, en même temps, le fait d'utiliser cette information induit le danger d'exposer les personnes concernées à des risques de discrimination ou d'atteintes à leurs droits et libertés, tout en mettant en jeu leur maîtrise sur leur image informationnelle. Il ne s'agit donc pas de soutenir que les traitements de données à caractère personnel seraient réglementés en raison du seul fait qu'ils concerneraient des données intimes ou cachées, même si l'intimité de la personne concernée est assurément un intérêt à protéger.

5. Par voie de conséquence, c'est à cet effet et dans cette optique que les traitements de données à caractère personnel doivent respecter toute une série de règles qui visent à atteindre un équilibre acceptable entre les intérêts en présence. A cet égard, si ce sont bien les intérêts du responsable du traitement et ceux de la personne concernée qui constituent les ressorts de la tension paradoxale sous-jacente à la réglementation des traitements de données à caractère personnel, il n'en demeure pas moins que ces deux catégories d'intérêts s'inscrivent dans un contexte plus global qui explique et justifie que soient également pris en compte les intérêts de la collectivité et des tiers considérés individuellement. Il s'ensuit que l'appréciation de la légitimité à traiter des données à caractère personnel implique de prendre en considération non seulement les intérêts du responsable du traitement et de la personne concernée, mais également ceux de la collectivité et des tiers considérés individuellement, sauf à isoler les deux premiers des contraintes de la vie en société.

II. Quel est le fondement juridique de la réglementation des traitements de données à caractère personnel?

6. Nous l'avons vu, l'objectif de la réglementation des traitements de données à caractère personnel obéit à la tension paradoxale qui la sous-tend. D'un côté, il faut permettre les traitements de données à caractère personnel. De l'autre côté, il faut tenir compte du sort de la personne concernée.

Dans ce contexte, la détermination du fondement juridique de la réglementation des traitements de données à caractère personnel consiste à dégager le fondement juridique dont peuvent se prévaloir les deux éléments constitutifs de cette tension paradoxale.

Du côté du responsable du traitement, le fondement juridique de son intérêt ([3]) doit être recherché dans ce qui justifie l'activité projetée à laquelle est liée la nécessité de traiter des données à caractère personnel. Ainsi, pour une entreprise, il s'agira dans la plupart des cas de la liberté d'entreprendre. Pour une collectivité politique, il s'agira de la réalisation de ses missions d'intérêt public.

18

De l'autre côté, la prise en compte du sort de la personne concernée dans le traitement des données à caractère personnel part du principe selon lequel l'individu a le droit de mener sa vie librement sans ingérence injustifiée, que ce soit à l'égard des autorités publiques ou des autres personnes privées. A cet effet, la personne doit être prémunie contre les risques de discrimination et d'atteinte à ses droits et libertés. Or, parmi les nombreux risques d'ingérence injustifiée qui sont susceptibles de peser sur les individus, ceux qui sont liés aux traitements de données à caractère personnel ont spécialement retenu l'attention en raison des développements considérables des nouvelles technologies de l'information et de la communication dans tous les secteurs d'activités, sans préjudice du danger déjà représenté par le fichage manuel des individus ([4]).

Le secteur des soins de santé n'a évidemment pas échappé à ce constat et, en la matière, la préoccupation majeure est de protéger la personne concernée contre les ingérences indues qui résulteraient du traitement de données à caractère personnel relatives à sa santé. Pour reprendre l'exemple de la communication «non autorisée» de données médicales, celle-ci est de nature à exposer le patient à des risques de discrimination à l'emploi, à l'assurance ou au crédit, tout en constituant une ingérence injustifiée dans sa maîtrise sur ce qui est su à propos de son état de santé.

([3]) Serait-il possible de dire qu'il est titulaire d'un droit ou d'une liberté à traiter des données?

([4]) Sur les risques présentés par les nouvelles technologies, voyez déjà: Council of Europe, T-PD, Report on the application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee, by J. M. DINANT, Chr. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, T-PD(2008)01, 11 January 2008; Council of Europe, T-PD, Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005); Council of Europe, Guiding principles for the protection of personal data with regard to smart cards (2004); Council of Europe, T-PD, Report on the application of data protection principles to the worldwide telecommunication networks, by Prof. Yves POULLET and its Team (2004); Council of Europe, Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003); Council of Europe, T-PD, Report on the protection of personal data with regard to the use of smart cards (2001), by Mr Karel NEUWIRT; Council of Europe, T-PD, Study contracts involving the transfer of personal data between Parties to Convention Ets 108 and third countries not providing an adequate level of protection (2001), by Mr. Jérôme HUET; Council of Europe, T-PD, Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, by Mr. Giovanni BUTTARELLI.

7. Traditionnellement, la protection de la personne concernée contre les conséquences néfastes des traitements de données à caractère personnel a été construite à partir du droit au respect de la vie privée ([5]). En effet, le droit au respect de la vie privée assure une protection générale à l'individu contre toute ingérence injustifiée dans la façon dont il entend mener sa vie. Cette protection générale de l'individu est fondamentale dans la mesure où elle permet l'exercice des autres libertés. En effet, sans cette liberté d'agir sans ingérence indue, les autres libertés n'ont que fort peu de signification ou d'intérêt.

8. Pour ce qui nous concerne, le droit au respect de la vie privée protège l'individu contre les ingérences, ou plus précisément, contre les risques de discrimination ou d'atteinte à ses droits et libertés, qui pourraient advenir à l'occasion du traitement de données à caractère personnel. La Cour européenne des droits de l'homme a déjà eu l'occasion de souligner l'importance de la protection des données à caractère personnel, et en particulier des données médicales, pour l'exercice du droit au respect de la vie privée, dans son arrêt du 25 février 2007 (Z. c Finlande) et dans celui du 27 août 2007 (M. S. c Suède). Dans ce second arrêt, la Cour a répété l'enseignement du premier selon lequel: 19

> «(...) la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général. La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé

([5]) Article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. La charte des droits fondamentaux de l'Union européenne (*J.O.U.E.*, 14 déc. 2007, C 303/01) énonce également que «*Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications*» (art. 7). Le Praesidium de la Convention qui a élaboré la Charte explique que les droits garantis à l'article 7 correspondent à ceux qui sont garantis par l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, mais que pour tenir compte de l'évolution technique, le mot «communication» a été substitué à celui de correspondance (Explications relatives à la charte des droits fondamentaux, *J.O.U.E.*, 14 déc. 2007, C 303/17, spéc. C 303/20). Sur le lien entre le droit au respect de la vie privée et la protection des données, voyez not.: H. BURKERT, «Dualities of Privacy — An Introduction to «Personal Data Protection and Fundamental Rights», Bruxelles, à paraître; S. CALLENS, «La «société de l'information»: une société de surveillance?», in M. MATHIEN (dir.), *La «Société de l'Information». Entre mythes et réalités*, Collection Médias, Sociétés et Relations Internationales, Bruxelles, Bruylant, 2005, p. 205; J. E. COHEN, «Privacy, Visibility, Transparency and Exposure», *The University of Chicago Law Review*, 2005, p. 181; C. JUGASTRU, «La protection des données personnelles et le commerce électronique — La situation en droit roumain», in Fr. PERON (coord.), *L'Europe dans la société de l'information*, Bruxelles, Larcier, 2008, p. 187; Th. LEONARD et Y. POULLET, «Les libertés comme fondement de la protection des données nominatives», in Fr. RIGAUX, *La vie privée. Une liberté parmi les autres?*, Travaux de la faculté de droit de Namur, n.° 17, Bruxelles, Larcier, 1992, p. 231; Y. POULLET, «Le fondement du droit à la protection des données nominatives: «Propriétés ou libertés», in *Nouvelles technologies et propriété*, Paris, Ed. Thémis, 1991, p. 175; «Data Protection between Property and Liberties. A Civil Law Approach», in *Amongst Friends in Computers and Law, A collection of Essays in Remembrance of Guy Vandenberghe*, Deventer-Boston, Kluwer Law and Taxation Publishers, 1990, p. 161; "La protection des données: entre libertés, droits subjectifs et intérêts légitimes", in *Liber Amicorum Paul Martens. L'humanisme dans la résolution des conflits. Utopie ou réalité?* Bruxelles, Larcier, 2007, p. 133; P. TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, Cahier des sciences morales et politiques, 5 tomes, Presses universitaires de France, 2000; Fr. RIGAUX, "La protection des banques de données et le respect de la vie privée", *rev. dr. ULB*, 1994, p. 51. M. VAN OVERSTRAETEN et S. DEPRE, «Le traitement automatisé de données à caractère personnel et le droit au respect de la vie privée en Belgique», *rev. trim. dr. h.*, 54/2003, p. 665.

qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention (...).»

9. Depuis lors, le droit à la protection des données à caractère personnel a été formellement consacré par la Charte des droits fondamentaux de l'Union européenne (6) dans une disposition distincte de celle qui concerne le droit au respect de la vie privée (7). Le Praesidium de la Convention qui a élaboré la Charte a énuméré les bases de cette nouvelle disposition. Parmi celles-ci se retrouvent l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ainsi que les principaux instruments juridiques européens qui ont été adoptés dans son giron pour assurer la protection des citoyens à l'égard des traitements de données à caractère personnel (8).

20 Il se confirme dès lors bien des précisions apportées par le Praesidium que ce droit nouvellement formalisé à la «*protection des données à caractère personnel*» s'enracine fermement et profondément dans le terreau du droit au respect de la vie privée et que le fait de l'avoir inscrit dans une disposition séparée n'a pas pour but ni pour conséquence de couper ce lien fondamental entre la règlementation des traitements de données à caractère personnel et le droit au respect de la vie privée. Il était particulièrement opportun de rappeler cette évidence (9).

III. Quel est le cadre juridique européen en matière de règlementation des traitements de données à caractère personnel?

10. En droit européen, la réglementation des traitements de données à caractère personnel a débuté par la Convention du Conseil de l'Europe du 28 janvier 1981 (10) et s'est poursuivie par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (11). Cette dernière indique d'ailleurs qu'elle

(6) La Charte des droits fondamentaux de l'Union européenne a été publiée au Journal officiel des Communautés européennes le 18 décembre 2000 (C 364/1). A son sujet voyez déjà: les communications de la Commission du 13 septembre 2000 sur la Charte (COM(2000) 559 final); du 11 octobre 2000 sur la nature de la charte (COM(2000) 644 final); du 27 avril 2005 sur le respect de la charte dans les propositions législatives de la Commission (Méthodologie pour un contrôle systématique et rigoureux) (COM(2005) 172 final); ainsi que les explications relatives à la Charte parue au Journal officiel de l'Union européenne le 14 décembre 2007 (C 303/17).

(7) Article 8 de la charte des droits fondamentaux de l'Union européenne:

«1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.»

(8) Explications relatives à la charte des droits fondamentaux, *J.O.U.E.*, 14 déc. 2007, C 303/17.

(9) En ce sens, Y. POULLET, "La protection des données: entre libertés, droits subjectifs et intérêts légitimes", o.c., p. 142.

(10) Conseil de l'Europe, Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens, n.° 108.

(11) *J.O.*, L 281 du 23 novembre 1995, p. 31. Pour une version compilée de la directive, consulter le document 1995L0046-FR-20.11.2003-001.001. Pour une présentation de la directive, voyez déjà: Y. Poullet, M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux et D. Moreau, «La protection des données à caractère personnel en droit communautaire», *Journal des Tribunaux de droit européen*, Bruxelles, Ed. Larcier, 1997, p. 121 et s. (en trois parties). L'adoption de la directive se base sur l'article 95 (anciennement 100 A) de la version consolidée du traité instituant la Communauté européenne. L'article 95.3 précise que, en matière de santé, de sécurité, de protection de l'environnement et de protection des consommateurs, la Commission prend pour base un niveau de protection

précise et amplifie les principes de la protection des droits et des libertés des individus, notamment du droit à la vie privée, contenus dans la Convention n.º 108 (12).

11. La directive 95/46/EC poursuit un double objectif dans son œuvre d'harmonisation des législations des Etats membres de la Communauté européenne: elle vise à permettre la libre circulation des données à caractère personnel, affirmée comme nécessaire à l'établissement et au fonctionnement du marché commun (13), tout en assurant le respect des libertés et droits fondamentaux des personnes (physiques) (14).

Pour éliminer les obstacles à la libre circulation des données à caractère personnel au sein du marché intérieur, il est apparu fondamental que les législations nationales soient harmonisées afin que tous les Etats membres offrent un niveau équivalent — mais élevé — de protection des droits et libertés des personnes à l'égard du traitement des données à caractère personnel (15).

Après cette harmonisation de leur législation en la matière, les Etats membres ne peuvent plus se prévaloir de raisons relatives à la protection des droits et libertés des personnes, dont le droit au respect de la vie privée, pour s'opposer à la libre circulation des données à caractère personnel. Il s'en déduit que, au regard de la directive, les Etats membres peuvent restreindre la circulation des données à caractère personnel pour des raisons autres que celles relatives à la protection des libertés et droits fondamentaux des personnes (16). Il va de soi que cette restriction doit être compatible avec les articles 95.8 et 95.10 du traité instituant la Communauté européenne et avec toute autre règle susceptible de s'opposer à une restriction à la circulation des données au sein des Etats membres ou du marché intérieur.

12. Aujourd'hui, si la directive 95/46/CE constitue le socle commun à tous les Etats membres de l'Union européenne en matière de réglementation des traitements de données à caractère personnel (17),

élevé en tenant compte notamment de toute nouvelle évolution basée sur des faits scientifiques. Elle ajoute que le Parlement européen et le Conseil doivent également s'efforcer d'atteindre cet objectif. L'article 95.8 prévoit que lorsqu'un Etat membre soulève un problème particulier de santé publique dans un domaine qui a fait préalablement l'objet de mesures d'harmonisation, il en informe la Commission, qui examine immédiatement s'il y a lieu de proposer des mesures appropriées au Conseil (voyez aussi l'article 95.10 pour l'insertion de clause de sauvegarde dans les cas appropriés pour permettre à un Etat membre de prendre des mesures provisoires soumises à une procédure communautaire de contrôle pour une ou plusieurs des raisons non économiques visées à l'article 30 du même traité — soit des raisons de moralité publique, d'ordre public, de sécurité publique, de protection de la santé et de la vie des personnes et des animaux ou de préservation des végétaux, de protection des trésors nationaux ayant une valeur artistique, historique ou archéologique ou de protection de la propriété industrielle ou commerciale —, sans que ces raisons puissent constituer un moyen de discrimination arbitraire ou un restriction déguisée dans le commerce entre les Etats membres).

(12) Considérant n.º 11 de la directive 95/46/CE.

(13) En ce sens et à ce propos, voyez déjà les considérants 3, 5, 6, 7 et 9 de la directive.

(14) En ce sens, voyez déjà les considérants 2, 3, 10 et 11 de la directive.

(15) Directive précitée, considérant 8. Voyez aussi l'art. 1 de la directive et son considérant 9.

(16) Comme l'ordre public ou les bonnes mœurs.

(17) La Cour de Justice des Communautés européennes a prononcé quatre arrêts importants en matière de traitement de données à caractère personne:

— C.J.C.E., 29 janvier 2008, Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU, affaire C-275/06;
— C.J.C.E., 30 mai 2006, Parlement européen v. Conseil de l'Union européenne et Commission des Communautés européennes, affaires jointes C-317/04 et C-318/04;
— C.J.C.E., 6 novembre 2003, Bodil Lindqvist v. Suède, affaire C-101/01;
— C.J.C.E., 20 mai 2003, Rechnungshof v. Österreichischer Rundkunf et

il faut cependant indiquer qu'elle est complétée par trois autres instruments:

— le règlement (CE) n.º 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ([18]);
— la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ([19]);
— et la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE ([20]).

Il faut aussi noter le fait que d'autres organisations internationales ont émis des instruments juridiques relatifs à la protection des données à caractère personnel, à l'instar du Conseil de l'Organisation de coopération et de développement économiques (OCDE) ou du Haut-commissariat aux droits de l'homme ([21]).

IV. Comment sont évalués les risques présentés par les traitements de données à caractère personnel?

13. L'évaluation des risques pour les droits et libertés des personnes concernées par les traitements de données à caractère personnel répond à un principe relativement simple: le risque ne dépend pas du contenu des données, mais bien du contexte dans lequel elles sont utilisées ([22]). Autrement dit, le risque dépend de la finalité poursuivie par le traitement des données à caractère personnel. Par conséquent, la dangerosité — tant potentielle que réelle — d'un traitement de données pour les droits et libertés de la personne concernée s'apprécie au regard de la finalité poursuivie par le responsable du traitement de données.

C'est la raison pour laquelle la notion de données à caractère personnel recouvre toutes les informations concernant une personne physique identifiée ou identifiable, et pas seulement les informations susceptible de révéler l'intimité des personnes con-

autres et Christa Neukomm et Joseph Lauermann v. Österreichischer Rundfunk, affaires jointes C-465/00, C-138/01 et C-139/01.

De même, le tribunal de première instance a prononcé deux arrêts intéressants en la matière:

— T.P.I., 8 novembre 2007, Bavarian Lager v. Commission des Communautés européennes, affaire T-194/04;
— T.P.I., 12 septembre 2007, Kalliopi Nikolaou v. Commission des Communautés européennes, affaire T-259/03.

([18]) *J.O.C.E.* du 12 janvier 2001, L 8/1.
([19]) *J.O.C.E.* du 31 juillet 2002, L 201/37. Pour la version consolidée, voyez le document 2002L0058-FR-03.05.2006-001.001.
([20]) *J.O.U.E.* du 14 avril 2006, L 105/54.

([21]) Respectivement, s'agissant de leur premier instrument juridique en la matière: Guidelines governing the protection of privacy and transborder flows of personal data on 23 Sept. 1980 et Guidelines for the Regulation of Automated Files containing Personal Data on 14 December 1990.
([22]) Rapport explicatif de la Convention n.º 108, considérant 43.

cernées. Par conséquent, toutes les informations, aussi banales que le numéro de téléphone ou le numéro d'une plaque minéralogique, sont des données à caractère personnel pour autant qu'elles concernent une personne physique identifiée ou (raisonnablement) identifiables. En effet, l'usage qui peut être fait de ces informations est susceptible d'exposer la personne concernée à des risques de discrimination et d'atteinte à ses droits et libertés, en ce compris la maîtrise de son image informationnelle, sans égard particulier pour la valeur du contenu de l'information. Le but de la directive 95/46/CE (la gestion des risques présentés par l'usage des informations relatives à des personnes physiques identifiées ou identifiables) explique cette définition de la donnée à caractère personnel ([23]).

14. Toutefois, cette manière d'évaluer les risques doit être nuancée pour les données dites «sensibles», ce qui inclut les données médicales. En effet, il est communément admis que le contenu informationnel des données «sensibles» augmente les risques de discrimination et d'atteinte aux droits et libertés de la personne concernée, en plus des risques liés à la finalité poursuivie par leur traitement. En d'autres mots, toute utilisation de ces données expose immanquablement la personne concernée à des risques plus grands d'atteintes à ses droits et libertés ([24]). C'est en ce sens que les données «sensibles» requièrent une protection particulière qui doit tenir compte tant de leur contenu informationnel que de la finalité poursuivie par leur traitement.

Dans cette logique, la directive a interdit le traitement des données «sensibles» ([25]) pour la raison que «*les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement (...)*» ([26]). Formulée différemment, cette interdiction représente la protection particulière voulue par la directive en ce qui concerne le traitement de données sensibles. Etant interdits, leurs traitements ne sont pas susceptibles de présenter un risque pour la personne concernée. C'est en quelque sorte l'application d'une politique de réduction maximale des risques présentés par les traitements de ces données. Mais cette interdiction de traiter les données sensibles ne doit pas être vue comme étant une exception à la libre circulation des données à caractère personnel. Cette interdiction est plus une limite qu'une exception à cette liberté de circulation. Autrement dit, la libre circulation des données à caractère personnel ne peut se concevoir que dans le plein respect des droits et libertés des personnes concernées et ce respect inclut l'interdiction de principe du traitement des données sensibles.

15. Après cette pétition de principe, la directive prévoit néanmoins une série d'hypothèses dans les-

([23]) Voyez le récent avis 4/2007 du 20 juin 2007 émis par le groupe 29 sur le concept de données à caractère personnel (WP 136). Au vu de cet avis, il est quand même permis de se demander ce qui ne constituerait pas une donnée à caractère personnel.

([24]) En ce sens: Rapport explicatif de la Convention n.° 108, considérant 43.

([25]) Directive 95/46/CE, art. 8.1.

([26]) Directive 95/46/CE, considérant 33. La Convention n.° 108 n'est pas aussi explicite. Elle dispose seulement en son article 6 que «*Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées.* (...)».

quelles l'interdiction de traiter les données sensibles ne s'applique pas ([27]). Dans ces hypothèses, la légitimité du traitement de données sensibles (son caractère admissible) est formellement présumée. En effet, ces hypothèses sont de nature à *justifier* une dérogation à l'interdiction de traiter les données sensibles, sans préjudice du respect des autres règles applicables aux traitements de données à caractère personnel. Il faut insister sur le fait que ces exceptions à l'interdiction de traiter les données sensibles doivent être strictement interprétées et qu'à défaut de correspondre à l'une de ces hypothèses, le traitement de données sensibles est interdit.

Dans chacune de ces hypothèses, le risque présenté par le traitement de données sensibles pour les droits et libertés de la personne concernée est considéré comme étant adéquatement maîtrisé. Il faut
24 immédiatement dire que ces hypothèses ne reposent pas sur une absence de risque, mais bien sur une mise en balance des intérêts en présence, ce qui requiert de mesurer les risques pour les droits et libertés des personnes concernées afin de pouvoir apprécier le caractère admissible du traitement des données sensibles.

16. C'est ainsi que la directive 95/46/CE autorise le traitement des données médicales dans sept hypothèses ([28]). Dans celles-ci, la légitimité du traitement des données médicales (la balance des intérêts en présence ([29])) est formellement présumée (cf. *infra* sur la nécessité de vérifier concrètement cette légitimité). Ceci s'explique par le fait que, en principe, les situations décrites dans ces hypothèses sont de nature à justifier le traitement de données médicales. Il faut rappeler que les exceptions à l'interdiction de traiter les données médicales doivent être interprétées de manière restrictive et qu'au-delà de leur champ d'application, il est interdit de traiter des données médicales.

C'est dans ce contexte qu'il faut apprécier la nature (c'est-à-dire les caractéristiques essentielles ou encore les propriétés) du consentement de la personne concernée à l'égard du traitement des données à caractère personnel relatives à sa santé.

V. Quelles sont les caractéristiques du consentement de la personne concernée dans le traitement des données médicales?

17. La première hypothèse qui permet de lever l'interdiction de traiter les données médicales est l'obtention du *consentement explicite* de la personne concernée à cet effet ([30]). La directive prend ainsi le parti de confier à la personne concernée le pouvoir d'autoriser le traitement des données médicales ([31]). A cet effet, il appartient à la personne concernée de mettre en balance les intérêts en présence et de pren-

([27]) Directive 95/46/CE, art. 8.2.

([28]) Directive 95/46/EC, art. 8. Sur l'interdiction de traiter et ses exceptions, voyez not.: J. HERVEG, "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in HealthGrid", in *Challenges and Opportunities of HealthGrids*, Studies in Health Technology and Informatics, vol. 120, Amsterdam, IOS Press, 2006, pp. 107-116.

([29]) Cf. *infra* pour l'identification de ces intérêts.

([30]) Directive 95/46/EC précitée, art. 8.2, *a)*.

([31]) Directive 95/46/CE, considérant 33. La directive ne donne pas d'indication formelle pour savoir s'il faut accorder un statut privilégié à cette base de légitimité pour le traitement des données «sensibles».

dre attitude en conséquence. Dans cette mesure, la personne concernée apprécie elle-même le risque présenté par le traitement des données médicales pour ses droits et libertés ([32]). Autrement dit, la directive considère que les risques pour les droits et libertés de la personne concernée sont présumés maîtrisés dès lors que celle-ci a valablement consenti au traitement des données médicales.

18. Cette attribution de pouvoir à la personne concernée représente incontestablement une expression forte de son autodétermination informationnelle — sa maîtrise sur l'information qui la concerne — ([33]). Elle peut aussi étonner; la personne concernée est-elle toujours en mesure de prendre une décision quand il s'agit des données médicales? N'est-il pas dangereux de s'en remettre à l'individu alors qu'il représente le plus souvent la partie «faible» ou à tout le moins en position de «demande», dans le cadre du traitement des données médicales? Par exemple, est-il possible pour un patient de refuser le traitement des données médicales à des fins scientifiques par le médecin qui le soigne? Comment s'assurer de la validité de son consentement pour qu'il ne se réduise pas à une pantalonnade? C'est pour tous ces motifs et afin de limiter les risques pour ses droits et libertés, que le consentement de la personne concernée doit répondre à un certain nombre d'exigences imposées par la directive.

19. C'est ainsi que le consentement de la personne concernée s'entend de «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*» ([34]). Cette définition demande à être développée.

D'abord, le consentement doit être indubitable.

Ensuite, pour être libre, le consentement doit être exempt de tout vice, de toute contrainte ou pression ([35]). Le Groupe 29 ajoute que le consentement «libre» désigne une décision volontaire, prise par une personne en pleine possession de ses facultés, en l'absence de toute coercition, qu'elle soit sociale, financière, psychologique ou autre ([36]). Il précise que le consentement donné sous la menace de privation de traitement ou de traitement de moindre qualité dans une situation médicale ne saurait être

([32]) Ce qui pose bien entendu la question de savoir qui prend en compte les intérêts des tiers et de la collectivité: le responsable du traitement, la personne concernée ou personne? Voyez *infra* à ce sujet.

([33]) Brièvement sur l'autodétermination informationnelle: Fr. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Paris, Bruylant, L.G.D.J., 1990, p. 588-589, n.° 532: «(...) *La juridiction constitutionnelle a déduit du droit de la personnalité l'un de ses attributs, à savoir: «le pouvoir reconnu à l'individu et résultant de la notion d'auto-détermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués (...) Cet attribut du droit de la personnalité est appelé «droit à la maîtrise des données personnelles» (...) Il n'est toutefois pas sans limite,* (...)». Voyez aussi: Conseil de l'Europe, Résolution 1165 (1998) du 26 juin 1998, *Droit au respect de la vie privée* (24e séance), point 5.

([34]) Directive 95/46/EC précitée, art. 2, *h)*.

([35]) A cet égard, le fait que la personne concernée puisse tirer un profit direct [par exemple, pour l'amélioration de son état de santé] ou indirect [par exemple, en participant au progrès de la science] du traitement de ses données médicales, ne vicie pas nécessairement son consentement. La perception d'une rémunération — au-delà de la simple couverture des frais éventuels — invaliderait-elle le consentement? Une réponse négative de principe ne semble pas devoir être adoptée. Tout dépend du cas d'espèce et de la manière dont le droit applicable a entendu protéger la personne concernée.

([36]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9. On pourrait néanmoins questionner la pertinence d'une définition aussi radicale notamment sur la possibilité de la mettre réellement en pratique.

considéré comme étant «libre» ([37]). Il ajoute encore que le consentement donné par une personne qui n'a pas eu la possibilité de faire un véritable choix ou qui a été mise devant le fait accompli ne peut être considéré comme étant valable ([38]). Le Groupe 29 rappelle qu'il considère que le recours au consentement comme base de légitimation d'un traitement de données doit être limité aux situations dans lesquelles la personne concernée est véritablement libre de son choix et a la possibilité ([39]) de retirer ultérieurement son consentement sans en subir de préjudice ([40]).

De plus, le consentement doit être spécifique et informé. Le caractère spécifique rappelle avec insistance que la personne concernée doit savoir exactement ce à quoi elle acquiesce, ce qui implique d'ailleurs nécessairement une information préalable adéquate. A défaut d'une information préalable et suffisante, le consentement de la personne concernée ne pourra pas être spécifique; il ne sera donc de toute façon pas valable. Toute la question réside alors dans le degré de précision de cette information dont le minimum est décrit aux articles 10 et 11 de la directive. Elle doit à tout le moins permettre la mise en œuvre de tous les aspects du traitement de données — qualité des données, droits de la personne concernée, mesures de sécurité et de confidentialité, notification à l'autorité de contrôle, etc. —. L'information doit aussi porter sur les conséquences du refus de consentir au traitement des donnés médicales.

Quoiqu'il en soit, l'information doit être d'autant plus précise et complète que le traitement porte sur des données sensibles comme les données médicales. En tout état de cause, la technique du blanc-seing est proscrite ([41]). Les exigences de spécificité du consentement et de son information préalable renforcent cette proscription. De même, les traitements ultérieurs incompatibles avec la finalité pour laquelle les données ont été collectées, sont interdits (art. 6, 1.b).

Il faut rappeler que le consentement peut être donné à l'avance, c'est-à-dire indépendamment du moment où les données sont collectées.

Enfin, le consentement de la personne concernée au traitement des données médicales doit être explicite ([42]). *A contrario*, le caractère explicite devrait exclure le recours au consentement implicite — quelle que puisse être la difficulté à définir cette notion —. A ce sujet, au-delà du caractère indubitable du consentement, son caractère explicite suppose qu'il s'exprime. Souvent, l'écrit signé qui le consigne en constitue la meilleure trace. Plusieurs législations européennes ont d'ailleurs ainsi traduit cette exigence. Cependant, d'autres actes de la personne concernée sont de nature à lui conférer cette carac-

([37]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9.

([38]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9.

([39]) Il s'agit en réalité d'un droit.

([40]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9. A nouveau, la formulation paraît excessive.

([41]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9.

([42]) Voyez: Directive 95/46/EC précitée, art. 8.2, *a)*, et le considérant 33.

téristique notamment au regard du contexte dans lequel ils sont posés. En effet, le consentement explicite peut s'exprimer au travers d'actions positives comme la participation à des recherches contre la maladie dont la personne concernée est atteinte, ou comme la demande d'être traité dans un service médical connu notoirement pour être un lieu de recherche. Le Groupe 29 considère à cet égard que si la personne concernée a la possibilité de refuser le traitement des données médicales mais qu'elle n'en a pas fait usage, cela n'équivaut pas à un consentement «explicite» ([43]). Il ajoute que le caractère explicite implique que le consentement doit porter en particulier sur la nature «sensible» des données médicales. Par voie de conséquence, la personne concernée doit avoir conscience du fait qu'elle renonce à une protection particulière ([44]).

La directive précise enfin que la législation d'un Etat membre peut prévoir que l'interdiction ne peut pas être levée dans certaines hypothèses par le seul consentement de la personne concernée ([45]). Ceci renvoie souvent aux règles relatives au secret médical.

20. Lorsque toutes ces conditions sont remplies, le consentement de la personne concernée permet de présumer la légitimité du traitement des données médicales en ce qui la concerne. On présume qu'elle a correctement effectué la balance entre ses intérêts et ceux du responsable du traitement et qu'elle a agi en conséquence. A défaut, son consentement ne pourra pas fonder le traitement des données médicales; il ne sera pas légitime de ce chef.

Il va sans dire que le consentement de la personne concernée ne dispense pas le responsable du traitement de données de poursuivre un intérêt légitime au regard des autres intérêts en présence [ceux de la collectivité et des autres tiers considérés individuellement]. De nouveau, le consentement de la personne concernée ne permet pas de couvrir le caractère illégitime ou illégal de la finalité poursuivie par le responsable du traitement.

21. Mais le consentement régulièrement octroyé est-il révocable? En règle, la personne concernée peut toujours retirer son consentement au traitement des données médicales, sans avoir à se justifier. Les conséquences de ce retrait sont controversées. Signifie-t-il simplement que, désormais, de nouveaux traitements ne pourront pas être possibles (sans toutefois remettre en cause ceux déjà mis en place sous l'empire du consentement), ou faut-il considérer en outre que les traitements de données effectués sur base du consentement initial ne peuvent plus être poursuivis? Dès lors que le consentement initial a été révoqué, la seconde hypothèse s'impose logiquement puisque le traitement de données initial n'a plus de base de légitimité. Mais ce n'est pas pour autant que les opérations passées deviennent illégitimes (il n'y a pas d'effet rétroactif au retrait du consentement). Elles ne peuvent simplement plus être poursuivies, sauf à pouvoir se prévaloir d'une autre source de légitimité.

([43]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 10.

([44]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 10.

([45]) Directive 95/46/EC précitée, art. 8.2, *a)*.

22. Au regard de ces développements, il n'est pas sûr que, considéré isolément, le consentement explicite de la personne concernée représente le fondement le plus solide (46) pour créer de grands réseaux télématiques dans les soins de santé ou de grandes bases de données médicales, et ce, même si le consentement de la personne concernée est régulièrement présenté comme étant la première base de légitimité pour le traitement des données médicales.

La directive prévoit heureusement d'autres hypothèses dans lesquelles l'interdiction de traiter les données médicales peut être levée sans recourir au consentement de la personne concernée. S'agissant de la finalité reprise dans ces hypothèses, il est aussi formellement présumé que le risque représenté par le traitement des données médicales pour les droits et
28 libertés de la personne concernée est correctement maîtrisé dans le cadre d'une mise en balance des intérêts en présence.

VI. Quelles sont les hypothèses dans lesquelles le consentement n'est pas requis pour traiter des données médicales?

23. L'interdiction de traiter les données médicales peut être levée lorsque «*le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates*» (47).

Il faut insister sur le fait que le traitement de données médicales doit être nécessaire à cette finalité, et pas seulement utile. Le responsable du traitement doit par conséquent pouvoir établir la nécessité de procéder à ce traitement pour respecter ses droits et obligations spécifiques en matière de droit du travail. Le traitement de données doit en outre être autorisé par une législation nationale qui doit prévoir des garanties adéquates pour la protection des données, sans que celles-ci ne soient autrement définies.

24. Le traitement des données médicales peut être admis dans le cas où «*le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement*» (48).

La notion d'intérêt vital vise expressément et exclusivement la situation de péril imminent à la vie d'une personne physique, qu'il s'agisse de la personne concernée ou de toute autre personne physique. Dans ce dernier cas, la directive précise que la personne concernée doit être dans l'incapacité physique ou juridique de consentir au traitement de ses données médicales au profit de cette autre personne. Il ne peut pas en être déduit que la personne concernée, capable physique et juridiquement de consentir, pourrait, sans autre forme de procès, refuser d'autoriser le traitement de ses données médicales

(46) Voyez déjà en ce sens le document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9.

(47) Directive 95/46/EC précitée, art. 8.2, *b)*. Cette finalité semble inclure la médecine du travail.

(48) Directive 95/46/EC précitée, art. 8.2, *c)*.

lorsque les intérêts vitaux d'une autre personne sont en jeu. Il conviendrait alors d'examiner la qualification à donner à ce comportement au regard du droit applicable.

Le Groupe 29 précise que cette dérogation ne peut en aucun cas être utilisée pour justifier le traitement de données médicales à d'autres fins que les soins à dispenser comme par exemple pour mener des recherches médicales générales qui ne donneront pas de résultats avant un certain temps ([49]).

25. Le traitement de données médicales peut être accepté si «*le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées*» ([50]).

Pour pouvoir se prévaloir de cette autorisation de traiter les données médicales, l'organisme doit poursuivre un but non lucratif et avoir un objet social qui concerne l'exercice de libertés fondamentales ([51]).

26. L'interdiction de traiter des données médicales peut encore être levée lorsque «*le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice*» ([52]).

Il faut insister sur le fait que, même manifestement rendues publiques, le traitement de ces données tombe toujours dans le champ d'application de la directive et que toutes les autres règles applicables à leur traitement doivent être scrupuleusement respectées.

27. La directive lève l'interdiction de traiter des données médicales dans une sixième hypothèse «*lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente*» ([53]).

L'hypothèse vise la finalité thérapeutique entendue largement ([54]), en ce compris la gestion de services de santé, ce qui devrait englober les finalités accessoires nécessaires pour assurer l'octroi de soins de santé, telles que la réception des patients, le secré-

([49]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 10.

([50]) Directive 95/46/EC précitée, art. 8.2, *d)*.

([51]) Directive 95/46/EC précitée, considérant 33.

([52]) Directive 95/46/EC précitée, art. 8.2, *e)*.

([53]) Directive 95/46/EC précitée, art. 8.3.

([54]) Quoique la directive semble ne viser que certaines fins relatives à la santé. Voyez à ce sujet la formulation du considérant 33. Le Groupe 29 dit que cette dérogation couvre uniquement le traitement de données médicales dans le but spécifique de fournir des services de santé à caractère préventif, diagnostic, thérapeutique ou de postcure et de gérer ces services de soins de santé, par exemple pour la facturation, la comptabilité ou les statistiques (Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 11).

tariat médical, les services informatiques, la facturation, la comptabilité ou les statistiques ([55]).

Par contre, cette hypothèse ne comprend pas les finalités de sécurité de sociale ou de santé publique, puisqu'elles sont reprises dans les exceptions pour motifs d'intérêt public important. De même, elle ne couvre pas l'hypothèse d'un traitement ultérieur non nécessaire à la fourniture directe de ces services, notamment l'utilisation des données pour la recherche médicale, le remboursement ultérieur des frais par un régime d'assurance maladie ou le recouvrement de créances ([56]).

En outre, le traitement des données médicales doit être effectué par un praticien de la santé, sans que cette notion ne soit autrement définie. Ce dernier doit être soumis par le droit national, ou par des règles adoptées par les autorités nationales compétentes, au secret professionnel ([57]).

A défaut d'être effectué par un praticien de la santé, le traitement peut être effectué par une autre personne si elle est soumise à une obligation de secret équivalente, notamment par voie statutaire ou par stipulation contractuelle.

On pourrait se demander si, dans cette hypothèse, le consentement de la personne concernée n'aurait pas été confondu avec le consentement aux soins prodigués? Le Groupe 29 a répondu sur ce point que l'acceptation de suivre un traitement médical ne constitue pas automatiquement un «consentement» au traitement des données médicales, en particulier en ce qui concerne leur communication ou transfert à un tiers ([58]).

28. Enfin, la directive permet aux Etats membres de prévoir d'autres hypothèses dans lesquelles les données médicales peuvent être traitées, à condition de pouvoir se prévaloir d'un motif d'intérêt public important ([59]), ce qui suppose la démonstration effective de son existence dans chaque cas d'espèce par l'Etat membre.

La directive visait principalement des motifs d'intérêt public important en matière de santé publique et de protection sociale «*particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie*» ([60]). Elle visait aussi la recherche scientifique et les statistiques publiques ([61]).

Les cas où les données médicales peuvent ainsi être traitées doivent être prévus soit par la législation nationale, soit par une décision de l'autorité nationale de contrôle.

Mais, dans ces hypothèses, les Etats membres ne peuvent autoriser le traitement de données médicales que sous la réserve de prévoir des garanties appro-

30

([55]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 11.

([56]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 11.

([57]) Voyez les développements à ce sujet dans le document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 12.

([58]) Document de travail adopté le 15 février 2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 9, note infra-paginale 10.

([59]) Directive 95/46/EC précitée, art. 8.4.

([60]) Directive 95/46/EC précitée, considérant 34.

([61]) Directive 95/46/EC précitée, considérant 34.

priés pour protéger les droits fondamentaux et la vie privée de la personne concernée (62). La directive ne précise cependant pas ces garanties.

En tout état de cause, les Etats membres doivent notifier à la Commission européenne les dérogations à l'interdiction de traiter les données médicales prises sur cette base (63).

VI. Qu'en est-il de la mise en balance concrète des intérêts en présence?

29. Il ne suffit pas de se prévaloir d'une des exceptions à l'interdiction de traiter les données médicales pour que le traitement de données soit légitime, même dans le cas du consentement de la personne concernée. En effet, il faut insister sur le fait qu'il ne s'agit que d'hypothèses dans lesquelles la légitimité du traitement de données est présumée. La légitimité du traitement de données — la mise en balance des intérêts en présence — doit en outre et surtout être vérifiée concrètement. Cette appréciation doit être menée avant la mise en œuvre du traitement de données et même après, le cas échéant, à intervalles réguliers en fonction des circonstances. En effet, la directive ne se contente pas d'une approche *a priori* et *formelle* de l'appréciation des risques pour les droits et libertés des personnes; ceux-ci doivent être appréciés *in concreto* et le cas échéant à intervalles réguliers durant le traitement. Ce constat vaut *a fortiori* lors du traitement de données médicales. Pour rappel, le niveau de sécurité technique et organisationnel est de nature à influer sur l'appréciation de la légitimité du traitement de données à caractère personnel.

30. En particulier, si le consentement valable et explicite de la personne concernée présume, jusqu'à preuve du contraire, l'existence d'un équilibre acceptable entre les intérêts en présence dans le traitement des données médicales, il paraît cependant difficile d'en déduire *de facto* la prise en considération adéquate des intérêts autres que ceux de la personne concernée, comme les intérêts de sa famille. A cet égard, si l'équilibre entre tous les différents intérêts en présence n'a pas été respecté, le traitement des données médicales sera illégitime, nonobstant le consentement régulier de la personne concernée.

Par contre, en présence d'une autre base de légitimité, obtenir en plus le consentement de la personne concernée est de nature à renforcer la légitimité du traitement des données médicales. C'est la raison pour laquelle il faut approuver et recommander fermement la pratique éthique qui consiste à agir en ce sens. Cette pratique se rencontre fréquemment dans le cadre des essais cliniques et dans le cadre de la constitution de réseaux télématiques dans le secteur des soins de santé. 31

31. Il faut rappeler que le responsable du traitement ne peut pas fonder le traitement de données médicales sur d'autres bases que celles énumérées ci-avant. Ceci exclut nécessairement le recours aux hypothèses de légitimation formelle énumérées à l'article 7 de la directive 95/46/EC pour les «simples» données à caractère personnel. Ainsi, par exemple, le responsable du traitement ne peut pas justifier le

(62) Directive 95/46/EC précitée, considérant 34.
(63) Directive 95/46/EC précitée, art. 8.6.

traitement de données médicales en effectuant une mise en balance des intérêts en présence, sans répondre à une hypothèse de légitimation du traitement de données médicales.

Avant de conclure sur la nature du consentement du patient dans le traitement des données médicales, il faut encore envisager brièvement la question des numéros d'identification et plus longuement la question des risques particuliers présentés par les traitements de données à caractère personnel.

VII. Qu'en est-il des numéros nationaux d'identification et des autres identifiants à portée générale?

32. Les États membres doivent déterminer les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement de données ([64]). En principe, les risques suscités par les identifiants ne proviennent pas de leur contenu mais bien des finalités pour lesquelles ils sont utilisés ([65]). A cet égard, la question de l'identification du patient et des professionnels des soins de santé est délicate. Elle doit néanmoins être résolue dans le cadre des projets de réseaux télématiques dans le secteur des soins de santé. Concrètement, le recours à des identifiants contextuels (spécifiques aux finalités poursuivies) représente une piste de réflexion intéressante.

32

VIII. Qu'en est-il des autres règles applicables aux traitements de données?

33. Même lorsqu'il est justifié par le consentement de la personne concernée, le traitement de données médicales doit respecter les autres règles applicables aux traitements de données telles que les autre conditions générales de licéité (les principes de qualité des données, de licéité, de loyauté et de durée de conservation des données), les droits de la personne concernée (droit d'accès, d'opposition et de rectification, droit à réparation et droit de ne pas être soumis à une décision individuelle automatisée et droit à un recours judiciaire), les obligations de confidentialité et de sécurité, et les obligations de notification à l'autorité nationale de contrôle.

En aucun cas, le consentement de la personne concerne ne peut dispenser le responsable du traitement de respecter les autres règles applicables aux traitements de données à caractère personnel en général et médicales en particulier.

IX. Comment sont gérés les risques particuliers présentés par les traitements de données à caractère personnel?

34. Si la directive 95/46/CE établit le cadre juridique commun aux Etats membres en matière de traitements des données à caractère personnel et fixe des règles spéciales pour légitimer le traitement

([64]) Directive 95/46/EC précitée, art. 8.7.

([65]) Voyez «Les numéros personnels d'identification: leur mise en œuvre, leur utilisation et la protection des données», une étude préparée par le Comité d'experts sur la protection des données (CJ-PD) sous l'égide du Comité européen de coopération juridique (CDCJ) (Strasbourg, 1991) et, mutatis mutandis, l'avis 2/2002 adopté le 30 mai 2002 par le Groupe de travail Article 29 sur la protection des données, relatif à l'utilisation d'identifiants uniques dans les terminaux de télécommunication: exemple de l'IPv6 (WP 5).

des données «sensibles», elle envisage en outre l'hypothèse dans laquelle, nonobstant le respect de cette double protection, certains traitements de données à caractère personnel sont quand même susceptibles de présenter des risques *particuliers* au regard des droits et libertés des personnes concernées (66).

35. En 1995, la directive précisait que, au regard de tous les traitements mis en œuvre dans la société, le nombre de ceux présentant de tels risques *particuliers* devrait être très restreint (67). Plus de dix ans après l'adoption de la directive et vu l'évolution des nouvelles technologies de l'information et de la communication, il n'est pas sûr que cette affirmation puisse être maintenue, surtout dans le secteur des soins de santé. Bien au contraire, aujourd'hui, le nombre de traitements présentant des risques particuliers pour les droits et libertés des personnes paraît plutôt très élevé, notamment en ce qui concerne les données médicales. En effet, depuis 1995, les évolutions technologiques ont permis la mise en place de larges réseaux télématiques dans le secteur des soins de santé pris au sens large, ces réseaux reliant des bases de données médicales substantielles sur une grande échelle (68), sans omettre le développement de bases de données génétiques également insérées dans des réseaux télématiques nationaux, européens voire, de plus en plus fréquemment, mondiaux. Tous ces développements n'ont-ils pas ouvert la porte à un nombre inouï de traitements présentant des risques particuliers pour les droits et libertés des personnes concernées?

36. Aux dires de la directive, les risques *particuliers* sont ceux qui résultent de la nature même du traitement poursuivi, de sa portée ou de ses finalités (69). Elle donne comme exemples des finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat (70). Ces risques particuliers peuvent aussi résulter de l'usage particulier d'une technologie nouvelle (71).

Traditionnellement, les exemples de traitements de données à caractère personnel présentant des risques particuliers sont ceux mis en œuvre par une autorité publique et portant sur l'ensemble ou une grande partie de la population (72) ou des traitements portant sur des données médicales (73). Les bases de données génétiques et les réseaux télématiques dans le secteur des soins de santé représentent autant de traitements de données susceptibles de poser des risques particuliers pour les droits et libertés des personnes concernées (74). Il faut déjà

(66) Directive 95/46/EC précitée, considérant 53.

(67) Directive 95/46/EC précitée, considérant 54.

(68) Le cas du réseau mis en place par l'EORTC ne manque pas d'interpeller, ainsi que ceux mis en place par les grandes firmes pharmaceutiques de par le monde.

(69) Directive 95/46/EC précitée, considérant 53.

(70) A propos des listes noires, voyez déjà: C. BURTON et Y. POULLET, «A propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires», note d'obs. sous C.P.V.P., avis n.° 09/2005 du 15 juin 2005, Belgique, Bruxelles, Larcier, *R.D.T.I.*, 2005/23, p. 102.

(71) Directive 95/46/EC précitée, considérant 53. L'utilisation des technologies Grid dans le secteur des soins de santé en constitue un bon exemple (voir à ce sujet: J. HERVEG, "Does HealthGrid Present Specific Risks With Regard To Data Protection?", in *From Genes to Personalized HealthCare: Grid Solutions for the Life Sciences*, IOS Publications, Studies in Health Technology and Informatics, 2007, vol. 126, pp. 219-228.

(72) Comme les recensements de la population.

(73) M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, o.c., *Journal des Tribunaux de Droit Européen*, 1997, p. 152, n.° 62. Ces exemples sont repris par: D. DE BOT (*Verwerking van persoongegevens*, Kluwer, 2001, p. 294, n.° 406).

(74) Le groupe 29 ne dit pas autre chose à propos de la création des systèmes de dossiers médicaux électroniques (document de travail adopté le 15 février

être attentif à la personne du responsable du traitement ([75]), à la sensibilité des données traitées, aux finalités poursuivies ([76]), à l'ampleur du traitement de données médicales, aux catégories de personnes concernées ([77]) et au respect des droits de ces dernières ([78]), sans oublier la question des flux transfrontières de données.

En bref, il faut être attentif à tout ce qui serait de nature à créer des risques particuliers aux droits et libertés des personnes concernées, sans pour autant faire basculer tous les traitements de données «sensibles» sous cette protection particulière complémentaire, et sans exclure *a priori* les traitements des «simples» données à caractère personnel, dès lors qu'ils sont aussi susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées ([79]).

34

37. Au regard du développement des réseaux télématiques dans le secteur des soins de santé, les risques particuliers sont surtout liés au fait que maintenant, les données médicales sont l'objet de plusieurs finalités, ce qui pose déjà la question de la possibilité de traiter des données médicales pour des finalités multiples, mais aussi la question de la détermination préalable, précise et concrète de ces finalités, sans omettre la question des traitements ultérieurs «éventuels». En effet, nous constatons aujourd'hui une tendance forte à ne plus définir de manière préalable et précise les finalités des traitements de données médicales, mais plutôt à organiser un système d'information en combinaison avec un système technique de sécurisation dont les finalités seront contrôlées *a posteriori*.

38. Autrement dit, on assiste à la création de systèmes d'information à deux niveaux. D'abord, on crée l'infrastructure du système d'information ([80]) et ensuite on va utiliser cette infrastructure pour réaliser toute une série de traitements de données à caractère personnel. Mais, fréquemment, on oublie que la création de l'infrastructure repose elle aussi sur des traitements de données à caractère personnel. En effet, il faut collecter et traiter des données à caractère personnel pour créer et faire fonctionner l'infrastructure du système d'information envisagé. Ainsi, par exemple, lorsqu'on crée un système d'information destiné à relier les hôpitaux et les médecins généralistes d'une même région, il faut d'abord constituer un registre permanent des hôpitaux, des professionnels de la santé et des patients. Ce n'est que lorsque ces traitements de données sont mis en œuvre qu'il est possible ensuite, dans un second temps, d'utiliser le réseau télématique pour transmettre de l'information dans le cadre de traitements de données

---

2007 par le groupe 29 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p. 23).

([75]) Par exemples, l'employeur traitant des données médicales ou génétiques, une société commerciale traitant des données génétiques.

([76]) Exclure les personnes concernées de certaines prestations ou de certains services, établir des profils individuels, collectifs ou semi-collectifs, les modes de financement des soins de santé. Nous pouvons également penser à la poursuite de finalités liées incompatibles entre elles (santé et commerce, par exemple).

([77]) Les mineurs, les personnes fragilisées, etc.

([78]) Le droit d'information, d'accès, de rectification, et d'opposition de la personne concernée.

([79]) Par exemple, les «listes noires» en matière d'assurances, de location d'immeubles, etc.

([80]) Comme pour les infrastructures de télécommunications *mutatis mutandis*.

particuliers comme les dossiers médicaux électroniques.

39. Dans les faits, nous constatons que la création de l'infrastructure du système d'information n'est plus perçue comme étant constitutive de risque pour les personnes concernées alors qu'en réalité, elle est à l'origine du risque. Elle constitue le premier traitement de données sur base duquel tous les autres traitements vont être construits. Or, il faut évaluer tant le premier risque (la création du réseau) que les risques liés aux finalités (secondes) des traitements de données. A cet égard, si le niveau de sécurité assuré par l'infrastructure contribue assurément à apprécier le risque créé par les finalités (secondes) des traitement de données, il n'est cependant pas exclusif de la prise en considération des autres critères pour apprécier la légitimité du traitement de données — qu'il soit au premier ou au second degré — surtout lorsqu'il s'agit de données sensibles comme les données médicales.

40. Ces systèmes d'information à étages et à finalités multiples posent d'ailleurs des problèmes au regard de l'exigence de la loyauté du traitement de données, dès lors que celle-ci renvoie à la nécessité de respecter les finalités (précises et concrètes) annoncées ainsi qu'à l'obligation d'informer la personne concernée. En effet, les multiples ramifications du système d'information ne sont pas transparentes, tant au niveau technique qu'au niveau des finalités, d'autant plus qu'elles sont évolutives (c'est la question de la boîte noire).

Cependant, les technologies de la communication et de l'information sont susceptibles de fournir des réponses à ces interrogations.

41. En droit, les Etats membres doivent préciser les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veiller à ce que ces traitements soient examinés avant leur mise en œuvre ([81]). Il ne faut pas s'y méprendre; la directive impose bien l'obligation ([82]) aux Etats membres d'identifier ces traitements particuliers et de veiller à leur examen avant leur mise en œuvre.

Pour rappel, le fait que les données médicales font déjà l'objet d'une protection particulière à raison de leur caractère sensible, ne les soustrait pas à la prise en compte de risques particuliers. Autrement dit, le traitement de données médicales qui présente des risques particuliers pour les droits et libertés des personnes concernées doit en outre faire l'objet d'un examen préalable.

42. L'examen préalable de ces traitements présentant des risques particuliers peut se dérouler de quatre façons.

Premièrement, il peut être réalisé par l'autorité de contrôle après la réception de la notification du traitement de données par le responsable du traitement ([83]). A la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données ([84]).

([81]) Directive 95/46/EC précitée, art. 20.1. Voyez cependant la formulation du considérant 53.

([82]) En ce sens: M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, o.c., *Journal des Tribunaux de Droit Européen*, 1997, p. 152, n.° 62.

([83]) Directive 95/46/EC précitée, art. 20.2.

([84]) Directive 95/46/EC précitée, considérant 54.

Deuxièmement, l'examen préalable peut être l'œuvre du détaché à la protection des données ([85]) qui, en cas de doute, doit consulter l'autorité de contrôle ([86]). A cet égard, la directive précise que celui-ci procède en coopération avec cette dernière ([87]).

Troisièmement, la directive prévoit que les Etats membres peuvent procéder à cet examen dans le cadre de l'élaboration d'une mesure du Parlement national qui définisse la nature du traitement et fixe des garanties appropriées ([88]).

Enfin, quatrièmement, les Etats membres peuvent aussi procéder à cet examen dans le cadre de l'élaboration d'une mesure fondée sur une telle mesure législative qui aussi définisse la nature du traitement et fixe des garanties appropriées ([89]).

X. Qu'en est-il des transferts de données à caractère personnel vers des pays tiers?

43. En règle, le transfert de données à caractère personnel faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si le pays tiers assure un niveau de protection adéquat, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la directive ([90]). Toutefois, sauf cas particuliers, le transfert de données à caractère personnel vers un pays tiers qui n'assure pas un niveau de protection adéquat peut être effectué notamment lorsque la personne concernée a indubitablement donné son consentement au transfert envisagé ([91]). Il existe d'autres hypothèses qui le permette sans requérir le consentement de la personne concernée ([92]).

Conclusions

44. Au terme de cette étude, il est possible de dégager les caractéristiques du consentement du patient au traitement de ses données médicales.

Nous avons vu que ce consentement n'était qu'une présomption d'équilibre entre les intérêts du responsable du traitement et ceux du patient. Dans cette logique, le consentement n'est pas tant une autorisation qu'une présomption de légitimité du traitement avec les intérêts, droits et libertés de la personne concernée, et que celle-ci peut être renversée.

De plus, fonder le traitement de données médicales sur le consentement du patient ne permet pas de faire abstraction des intérêts de la collectivité et des

([85]) Le détaché à la protection des données à caractère personnel est une personne désignée par le responsable du traitement, conformément au droit national auquel ce dernier est soumis, et qui est chargée notamment:

— d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive,
— de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 21.2,

et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées (art. 18.2 de la directive).

La présence d'un détaché à la protection des données permet aux Etats membres de prévoir des simplifications ou des dérogations à l'obligation de notifier les traitements de données à caractère personnel à l'autorité de contrôle (art. 18.2 de la directive).

([86]) Directive 95/46/EC précitée, art. 20.2.

([87]) Directive 95/46/EC précitée, considérant 54.

([88]) Directive 95/46/EC précitée, art. 20.3.

([89]) Directive 95/46/EC précitée, art. 20.3.

([90]) Article 25.1 de la directive 95/46/CE. L'article 25.2 précise ce que l'on entend par niveau de protection adéquat.

([91]) Ce consentement a un double objet; d'abord sur la finalité poursuivie, ensuite sur le transfert.

([92]) Voyez l'article 26 de la directive 95/46/CE.

tiers considérés individuellement. Par voie de conséquence, la légitimité de leur traitement requiert de les prendre également en considération.

Surabondamment, il peut arriver que le consentement du patient ne suffise pas à légitimer un traitement de données. La directive prévoit d'ailleurs expressément cette dernière hypothèse.

Par ailleurs, nous avons vu qu'il existe des hypothèses dans lesquelles l'interdiction de traiter des données médicales est levée sans qu'il soit besoin d'avoir recueilli le consentement du patient.

En tout état de cause, le consentement du patient n'est pas suffisant pour permettre le traitement de données médicales. En effet, il ne dispense pas le responsable du traitement de respecter l'ensemble des autres règles applicables aux traitements de données médical telles que les autres conditions générales de licéité (les principes de qualité des données, de licéité, de loyauté et de durée de conservation des données), les droits de la personne concernée (droit d'accès, d'opposition et de rectification, droit à réparation et droit de ne pas être soumis à une décision individuelle automatisée et droit à un recours judiciaire), les obligations de confidentialité et de sécurité, et les obligations de notification à l'autorité nationale de contrôle.

Le consentement n'est pas plus suffisant en présence de traitements de données médicales qui présentent des risques particuliers pour les droits et libertés du patient. A l'instar du respect des autres règles applicables aux traitements de données à caractère personnel en général et médicales en particulier, cette dernière situation démontre que d'autres éléments interviennent pour apprécier la légitimité d'un traitement de données à caractère personnel que le seul consentement de la personne concernée.

Il s'ensuit que le consentement est loin d'être l'expression d'une maîtrise-appartenance du patient sur les données à caractère personnel relative à sa santé et, de la même façon, il n'est pas non plus l'expression d'une relation contractuelle avec le responsable du traitement.